Privacy & Security Tiger Team
Draft Transcript
February 4, 2011

Presentation

Judy Sparrow – Office of the National Coordinator – Executive Director
Good morning, everybody, and welcome to the Privacy & Security Tiger Team Call. The call will run from 10:00 to noon, Eastern Time. It's a Federal Advisory Call, so there will be opportunity at the end of the call for the public to make comment. Workgroup members, please remember to identify yourselves when speaking.

Let me do a quick roll call. Deven McGraw?

Deven McGraw – Center for Democracy & Technology – Director
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Paul Egerman?

Paul Egerman – Software Entrepreneur
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Latanya Sweeney? Gayle Harrell? Carol Diamond?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Judy Faulkner? David McCallie?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Neil Calman? He did dial in.

Deven McGraw – Center for Democracy & Technology – Director
Yes. I know I heard him too.

Judy Sparrow – Office of the National Coordinator – Executive Director
Yes. David Lansky? Dixie Baker?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I'm here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Micky Tripathi? Rachel Block? Christine Bechtel?

Alice Brown – National Partnership for Women & Families – Director HITP
This is Alice Brown. I'm on for her.

Judy Sparrow – Office of the National Coordinator – Executive Director
Yes. Right. Thank you, Alice. John Houston could not make the call. Wes Rishel? Leslie Francis also could not make it. Lisa Tyro is on. Adam Green?

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Joy Pritts is coming in late. Did I leave anyone off? Okay. I'll turn it over to Deven and Paul.

Deven McGraw – Center for Democracy & Technology – Director
Great. Thank you, everyone. Thank you to members of the tiger team for joining us today. Thank you also to members of the public, who are signed on and listening to the call today. We very much appreciate your paying attention to these issues.

The agenda that we're going to cover today is to sort of start off with a little debrief of the presentation of the patient matching recommendations to the Policy Committee, which went very well. Then we'll move into a discussion of the intersection of the recommendations that are in the PCAST Report with the tiger team recommendations that we have already teed up for the Policy Committee. Paul Egerman will talk a bit in that section about sort of what the purpose of the PCAST Workgroup is so that we have a clearer sense of what we want to accomplish in terms of our own discussion of how our recommendations intersect with what PCAST has said.

Then we'll take a little bit of time to talk about the schedule ongoing and what issues we're going to take up in the immediate term. There will be opportunity to give us feedback, largely off-line so we can continue to move the discussion forward on issues when we have time on the call. But we want to get your input about some of the issues that we have not really taken up yet in order to finish up the population of a framework of privacy and security policy recommendations. So I want to just basically introduce to you a document that is a bit of a gap analysis and then invite you all to give us feedback. Then we hope to spend the second hour of the call beginning a conversation about user authentication.

With that we'll move into just a brief debrief, the repeat of the recommendations to the Policy Committee. They were adopted without modification, so there was a lot of good dialogue back and forth about, in particular, why we didn't set a specific level of accountability for matching accuracy. We had some good discussion about that, but the Policy Committee liked the direction that we were heading in with these recommendations and so we were quite pleased with that.

Paul, I don't know if you want to add anything or anybody else on the call, who was present at the meeting or listening in.

Paul Egerman – Software Entrepreneur
I think, Deven, you did a good job of summarizing the Policy Committee meeting. It went well. Paul Tang raised an interesting issue. He was concerned about exposure of information when you actually searched for an individual, if you did like a name search. We responded by saying that was not part of the issues that we address in the patient matching, but other than that I thought the presentation went very well. Neil was present. I don't know if other people have any comments.

Deven McGraw – Center for Democracy & Technology – Director
Yes. Paul, on that particular comment—thank you for reminding me about that one—I did note that the concept of a patient record locator service or some sort of mechanism for locating patient records. I think the issue that Paul Tang raised about how much data gets exposed in that index is one that is probably best nested in a discussion about that particular set of issues.

Paul Egerman – Software Entrepreneur
It's a good issue and it's an interesting issue.

Deven McGraw – Center for Democracy & Technology – Director
Yes.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
If I could just comment? I didn't listen to the Policy Committee call, but I think it's more than a good issue. I think it's a critical issue, because a lot of people who put together record locator services, not intentionally, I think don't really appreciate the issue that Paul is raising. At least in the way that we develop policy from the context of the common framework the ideal is that the index does not give you back more than you already know when you put in to look for a patient and does not expose, unintentionally, issues. But I do want to say that that particular set of issues just around a record locator services nested in a larger set of policies that I want to make sure don't fall off the radar, which is around what happens when you do get the wrong information back and what are the policies for that kind of unintended disclosure.

Deven McGraw – Center for Democracy & Technology – Director
Right. Good point, Carol. Anybody else on the Policy Committee presentation before we move into the PCAST discussion? Okay. With that, Paul, take it away.

Paul Egerman – Software Entrepreneur
Sure, if we could ask them to load up the PDF that says, "PCAST Analysis."

Deven McGraw – Center for Democracy & Technology – Director
Yes. Do they? Okay, they can load it. Look at that.

Paul Egerman – Software Entrepreneur
I wish life was always like this; you ask for something and it just happens. This is a document and we apologize that you didn't get this a little bit sooner. It's a document that was prepared. I think it was Linda Koontz from MITRE put it together. She really did an excellent job on a very interesting challenge. I want to sort of explain what the document is and do my best to frame the discussion. What she tried to do was look at the PCAST Report and compare what it says in the PCAST Report against the tiger team recommendations that have been made so far. That's an interesting challenge because the best way to describe it is it's almost like we're speaking different languages at times. In other words, we refer to something in one way and PCAST refers to it in a different way, so she did her best to come up with a way to categorize and cross reference what PCAST has done.

The purpose of this document and discussion is really to feed information into the PCAST Report Workgroup. There is not like a super deadline for it. What I want to do in this discussion is walk you through it, but also then give you a chance to, if you choose to, to go through it in greater detail and forward back to us more detailed comments that you might want to make. Again, to frame the discussion, it's a comparison against what's in the PCAST Report and the recommendations that we've already made. The discussion is not about things that are in the PCAST Report that we haven't yet addressed. For example, the PCAST Report talks about research and there are probably a lot of people that have opinions about what it says about research. Those are all valid opinions, but that's just not part of this discussion. This is just a discussion of to what extent is what we've done so far in this tiger team consistent or inconsistent with the PCAST Report.

The basic structure that Linda put together, which is really excellent, is they put together three columns. It says, "PCAST Finding." The second column is Tiger Team Recommendations. The third column is her analysis. Then she did her best to come up with categories or subject headings, like Fair Information Practices, which it's not referred to with that terminology within the PCAST Report, so she read through it. She found a section that she felt was appropriate in this. She put down what it says in the report. She put down a page reference. In the second column, she repeated our recommendations and then she did her analysis.

Now, in putting this together I also want to explain my role. I think some people know I also chair the PCAST Report Workgroup, but in that role, I am trying to do my best to be neutral. In other words, it's not like I particularly have a strong opinion one way or another or am trying to express a strong opinion one way or another on any of these particular topics. I'm simply trying to get the information put together. As I said before, sometimes I have this habit that when somebody puts like a PowerPoint presentation for me to sell whatever is on the PowerPoint presentation, but that's not what I'm trying to do in this discussion. I'm just saying this is what she said the purpose is. This is like a .... Do we agree with that? If so, great; if we don't that's great too. Also, as we go through this are there sections that are missing here? In other words, she did a really good job of laying out what I think were the critical things, but maybe there's something that was missed here. If so, that's important to know.

What we want to do in this discussion is take you through the report, but we're going to make it time limited. We're going to do 30 or 40 minutes going through this report and this analysis, hear your comments, but it's really to start the discussion so that people feel comfortable thinking about these issues and providing this feedback. I think we'll ask for feedback in about a week if that's comfortable. The way you give feedback is you take the Word document and do correct changes and send it to Deven and me and, if you want to, the rest of the tiger team.

Before I start walking through the actual analysis does anybody have any comments or questions about the way I tried to frame the discussion?

Deven McGraw – Center for Democracy & Technology – Director
Yes, Paul. I just want to be clear that the audience for this analysis when we finish it is the PCAST Workgroup.

Paul Egerman – Software Entrepreneur
That's correct.

Deven McGraw – Center for Democracy & Technology – Director
Okay. To inform their discussions about sort of implementation options—

Paul Egerman – Software Entrepreneur
Yes and the reason for that is when the workgroup was formed Dr. Blumenthal requested that all of the workgroups funnel their information through that workgroup so that we not have various workgroups independently reporting information to the Policy Committee. He wanted it to come from one place, all in one shot, so that was the reason why, which makes sense.

Deven McGraw – Center for Democracy & Technology – Director
Yes.

Paul Egerman – Software Entrepreneur
So the first one says, "Fair Information Practices," you can read what it says there. It quotes something on page 46. Then in the second column, it repeats the wording, some of the wording from our August 19th letter. It starts—it's fortunate sometimes you start with something that seems very general, that's a very general statement and the analysis says, "The recommendations appear consistent with PCAST observations." Does anybody have any comment on this?

Deven McGraw – Center for Democracy & Technology – Director
Yes, I think that's right. It's Deven. I mean there are sort of more general, overarching policy statements, which are important, but it's good that they're consistent.

Paul Egerman – Software Entrepreneur
Yes. It starts with a few very general statements and then you get, in another page, to some more specifics. Clear data rules really cite the same page. We had some very general statements about building and maintaining public trust. Then in this document, it cites, from the same letter, but basically more detail about what we said about limitations on collections and use. The analysis here says, "Tiger team recommendations appear consistent. Tiger team recommendations provide further detail, which is what you would expect."

I don't know if anybody has any observations about this topic.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
The only observation I would make, which maybe for those that haven't read the PCAST Report is that the quote from page 46, interestingly doesn't include the word exchanged, although the PCAST Report itself is highly biased toward exchange. So I think that's important to know; that even their focus on exchange is consistent with our tiger team's.

Paul Egerman – Software Entrepreneur
That's a good, excellent observation, Dixie. One of the things that's difficult sometimes reading the PCAST Report is that it was apparently written by people who don't work in the health IT industry the same way we all do, so some of the words that they use may have meaning that we might view differently. So you used the word exchange; I think we know what we mean by exchange. We mean that means from exchanging information, in my mind, from one organization to another organization. But I'm not sure that that's necessarily the way the PCAST authors meant information exchange. I mean I don't know. It's an interesting observation.

That was a comment that was good about clear data rules.

Deven McGraw – Center for Democracy & Technology – Director
Yes.

Paul Egerman – Software Entrepreneur
The next one is transparency. Basically, again, they cited a couple of pages in the PCAST Report saying the patient cannot make meaningful choices unless he or she understands the flows and uses of information. Then again, they cited one of our letters where we made a recommendation about transparency in a lot more detail. We talked about a layered notice process, although I would make the additional observation that this tiger team recommendation on transparency has not yet been approved by the Policy Committee. That's sort of an administrative observation.

Then we have the observation that the recommendations appear consistent and more detailed than PCAST, although the results of this observation that's very important that the tiger team place greater emphasis on the role of the provider in educating patients.

Any comments there? So I'm interpreting silence as either everybody agrees or, alternatively, I erroneously still have my phone on mute and nobody can hear what I'm saying.

The next subject, this is when you start to get to the patient/provider choice; in my mind, perhaps there are a few more challenges. But on the first column, on the PCAST column it talks about this concept of the DEAS (Data Element Access Services), which is really a patient locator service or a data element locator services. In the report it says that patients have the right to restrict the types of data elements indexed and could opt-out—and they did use the expression opt out, as it's described here—of the DEAS completely. When they use the expression opt out I don't necessarily think that they meant that in the same way we think of opt-in and opt-out, but that's hard to know.

They also made a comment about using meaningful use to incentivize providers and options of tagged data elements. This is an area then that we put a lot of effort into it and I think the tiger teams at first were really great, but in the middle column, you see a description of what we did with meaningful consent and making sure that meaningful consent had to be provided before a provider releases control over exchange decisions.

The third column on this issue: It says the recommendations are consistent, but it does make the note that we specified that consent must be provided before the provider releases control and the PCAST position of the timing is unclear as to when the timing would occur.

So what observations or comments does anybody have about this? Do you agree with what's written here? Does anybody have anything they want to say about this topic?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I'll chime in here, Paul. I think this is a great analysis by the way. I don't know who did it—

Paul Egerman – Software Entrepreneur
Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
But my compliments. I think this where we see the emergence of the PCAST focus at the data element level—

Deven McGraw – Center for Democracy & Technology – Director
Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
And that intersects with our tiger team work in my mind with respect to the work we did last year on consumer choice at the data element level and our conclusion that neither the market, nor clinical operations for that matter were ready for really choice at the data element level. Our work has been focused clearly at a much less granular level than the PCAST seems to be targeting.

Paul Egerman – Software Entrepreneur
That's an excellent observation, Dixie. Actually, we do have granular consent coming up in this document, although one could make that observation also in the analysis section that the tiger team's comments on consent were not based upon granular consent—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. I'm really focusing. That first bullet you have there under the blue where it says, "Patients would have the right to restrict the types of data elements indexed at all,"—

Deven McGraw – Center for Democracy & Technology – Director
Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's where I was referring to.

Deven McGraw – Center for Democracy & Technology – Director
Okay.

Paul Egerman – Software Entrepreneur
I think that's a great observation, Dixie.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I would echo Dixie's observation. I realize that our goal here isn't to react to the PCAST Report per se, but I think this is one of the central issues that will get more discussion as PCAST is vetted in the hearings that are coming up in a couple of weeks around the distinction between preserving the information at the granular level. And in addition, preserving a broader context of the documents that these items are indexed from. I think it's a little bit naïve to specify that you could opt-out of indexing at the granular level without saying something about the broader context. Does that mean the whole document that that information came from is now restricted or does that mean that you ... holes in the document, like a CIA operative would. Some of those things are going to be problematic in the actual implementation of something like this, but I agree with the recommendations here. I think it's captured well. I just think that there is a lot more that needs to be said in the long-run.

Paul Egerman – Software Entrepreneur

Yes. Excellent observations, David. The interesting challenge—and maybe you or somebody can tell us how to meet this challenge—is when we go through this item-by-item the analysis, so far people are agreeing with the analysis, but there are issues like what you just described that may not be really captured in this analysis. So the challenge is to figure out how to write that down and articulate it, but those are important issues. Again, we want to keep ourselves constrained to the concept that we're not talking about sort of like issues that we haven't yet addressed, but we want to be clear that the tiger team really wasn't addressing the granular consent and there may be other issues related to the types of granular consent that are suggested by DEAS.

Deven McGraw – Center for Democracy & Technology – Director
Yes. We did say some things about granular consent. We've just got that on another line.

Paul Egerman – Software Entrepreneur
Okay. So that's great.

Deven McGraw – Center for Democracy & Technology – Director
One other thing that I just thought about is where they are applying the patient's right to consent in this particular context is for a kind of query model that is similar, if not the same as the trigger circumstances I think that we defined in the letter. Do people agree with that? It's an application of consent to whether or not the data can be accessed or indexed in a DEAS. It's sort of similar to some of the trigger situations that were examples in our letter I think.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I don't agree, because they stress, PCAST stresses that DEAS never has any clinical information; it only has the indexes and pointers and it does linking, but it never has actual data.

Deven McGraw – Center for Democracy & Technology – Director
Well, although the person's name is data. The name in an index and even if the index just identifies the location of records there are health implications associated with that.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Right. That's a good point. I would think you talked about federated HIEs or intermediaries is the term we were using. Yes. That's very similar to DEAS. You're right. Yes.

Deven McGraw – Center for Democracy & Technology – Director
Yes. So rather than opining as to whether it's the same or similar I think we could just note here about where the tiger team's approach to consent with respect to directed exchange versus trigger situations and draw that to the PCAST Workgroup's attention.

Paul Egerman – Software Entrepreneur
Yes, because that's a great observation—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Paul Egerman – Software Entrepreneur
As I think about what you said, Deven, I would tend to agree. The DEAS is structured more of a query situation where you can sort of assemble information that you might want to obtain. That is actually different than a fair percentage of what we did with the … team, which was much more directed exchange, referrals, transitions of care, CCD kinds of things, which is more consistent with stage one of meaningful use.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I would also come back to what Dixie said a minute ago about the notion of exchange. The PCAST model is based on kind of a master index of records in place that allow someone to request an exchange to occur. In other words, you go find the existence of something before anything has been exchanged

and then you say, “That’s what I want. Can I get it?” At which point you either can get it or not and you can get the key to decrypt it or not. So it’s kind of a different approach. Theoretically, it exposes a lot of data before any so-called exchange might happen.

Deven McGraw – Center for Democracy & Technology – Director
Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
So I think this question here around—I like the language that she used here, “Release control.” That’s the operative word. Does someone have access to this data from the outside even though it hasn’t actually exchanged yet is the question. So is the data exposed for the purposes of look-up is the trigger. It kind of forces us to refine our definition of trigger.

Deven McGraw – Center for Democracy & Technology – Director
Yes.

Paul Egerman – Software Entrepreneur
Right.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
And control. Yes.

Paul Egerman – Software Entrepreneur
That’s true, although to be clear, my reading of the PCAST Report is the data element index is not necessarily exposed. There’s a federated model that you get with an HIE that is like a record locator model that did nothing more than say here’s a pointer to, say, Dr. Smith and then when you go to Dr. Smith’s site that’s when you find the data element index.

Deven McGraw – Center for Democracy & Technology – Director
Oh.

Paul Egerman – Software Entrepreneur
I think that that would be allowed within the PCAST.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
That might be allowed, but I don’t think that’s how most people are reading it. I think they’re reading it like a Google search engine—

Paul Egerman – Software Entrepreneur
That’s true.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Where you have some kind of a centralization of index information, centralization being whatever scale you want—it could be regional or IDN or statewide or whatever, but there is some degree of centralization of index information that is exposed to let the querier find out if there’s something of interest. At which point then the exchange could occur where they get an actual copy of the original data.

Paul Egerman – Software Entrepreneur
Well, yes. This is a good discussion, but actually, I think the very next topic is granular choice, so I’m going to just pull that up as we continue this discussion.

Deven McGraw – Center for Democracy & Technology – Director
Yes.

Paul Egerman – Software Entrepreneur
First, we go to meaningful consent and then we do granular consent.

Deven McGraw – Center for Democracy & Technology – Director
Right.

Paul Egerman – Software Entrepreneur
So in terms of better informed, meaningful consent, again, it's amazing that Linda in MITRE was able to pull this together. This was a lot of work. They siphoned sections of the PCAST Report. She repeated back the major bullets of meaningful consent and this is what she said. I mean we are focused on consent with regards to participation in health information exchange. It says, "Consistent with the PCAST observations." It says, "As noted above, is not clear." That patient may be able to make a choice about whether or not their data is indexed in advance, but it was clear from our recommendations that would be the case. We provide more details on what makes choice meaningful.

Do people have any initial observations about this?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Paul, I'm joining the call late and I haven't got the thing up on the screen yet, but in saying we've emphasized what makes choice meaningful one of the issues we've discussed substantially is the effect on transmission of the information from the original source vis-à-vis consent, in other words, two models of consent. One is it's okay to send it somewhere, as long as it's never retrieved. In other words, we trust the central source fully to implement the permission. The other is it shouldn't leave the provider. Is that listed as a difference between our view and theirs?

Deven McGraw – Center for Democracy & Technology – Director
Wes, I don't know when you joined the call, but we did have a discussion about how our recommendations on meaningful consent do make a distinction between types of exchange models that our trigger-types of situations are similar to the DEAS type of model, which is the overwhelming focus of the PCAST Report.

Paul Egerman – Software Entrepreneur
Yes. It almost seems like—

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
My bad for—

Deven McGraw – Center for Democracy & Technology – Director
No. No. That's okay. You have the same or similar observation I think if I heard your comment correctly, so that's good.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Well, my initial impression is that the PCAST Report is not clear on that point, so if that's the impression you have, then fine. I was not able to get any; I mean there's a sense of getting data from the source in the PCAST Report, but I wasn't able to infer from that that it was against centralizing at all and that it had any different implications on privacy for doing it, but I'll go back and check the transcript later.

Deven McGraw – Center for Democracy & Technology – Director
Okay.

Neil Calman – Institute for Family Health – President & Cofounder
Can I make a comment on this issue? This is more than a technological issue and I think this is one of the things that you've heard concerns about before. But even if the technology could figure out how to tag and people could figure out a mechanism to consent to every different type of data, some of those things could be used to be potentially misleading to future providers at worst. At best, could be seen as

providing incomplete information that could potentially be dangerous to patients in ways that they might not even appreciate, so intentional misuse could be trying to keep data on medications that people have been given in a particular drug class and then be prescribed medications that potentially interact. The ability to get multiple controlled substances so that people could hide the fact that they're getting them from another provider all of the way to just much more innocent stuff about people saying, "Well, I really don't want people to know that I'm on these mental health medications." And not knowing that by doing so that those things are potentially dangerous to people with cardiac conditions and to people, who are taking other medications.

So my concern here is there has got to be a way clinically to introduce some intelligence that I don't think exists yet that would inform patients at the point that they're choosing not to consent to particular types of information as to what the potential dangers of that are. We can't even figure out how to develop decision support yet for interactions that are meaningful to think about the intelligence that would need to be built into these systems to do that, to inform people at the time they're consenting about the potential implications of their consent procedures, to me that technology is not getting developed. So I still have tremendous concerns about this granular consent stuff.

Paul Egerman – Software Entrepreneur
Neil, those are excellent observations. It sort of takes us—I scrolled down on the screen—to the topic of granular consent. This document cites page 46. There's a fair amount of information about sort of the granular nature of what is recommended. The middle column talks a little about what we said. The main thing we said is I think what you're saying, Neil, which is we could query the technologies for supporting granted consent. It's promising, but it's still in the early stage of development that there are some interesting issues that need to be worked out.

Neil Calman – Institute for Family Health – President & Cofounder
But to go back to your original statement for why we're doing this, we're doing this because the consumer of our discussion today should be the PCAST—

Paul Egerman – Software Entrepreneur
Right.

Deven McGraw – Center for Democracy & Technology – Director
Yes, PCAST Workgroup, not PCAST.

Neil Calman – Institute for Family Health – President & Cofounder
Right. Well, the PCAST Workgroup, so my recommendation is that we include a significant caution here, again, that this is not just a technological issue and that at least on the provider side I can tell you and I don't know with the consumer side. I know people have been pushing for more granular consent to be possible. I think in some cases it makes perfect sense to do that. But on the provider side I can tell you that every single provider is terrified of this.

Deven McGraw – Center for Democracy & Technology – Director
Yes.

Paul Egerman – Software Entrepreneur
Yes, I know. And there's—

Neil Calman – Institute for Family Health – President & Cofounder
And I would love to figure out a way to combine the consumer concerns with the provider concerns and actually be able to say something intelligent about this—

Deven McGraw – Center for Democracy & Technology – Director
Yes.

Neil Calman – Institute for Family Health – President & Cofounder

And about what's possible, because if we don't do that this is going to be like a dialogue that's not going to really move this discussion forward in any way.

Deven McGraw – Center for Democracy & Technology – Director
Yes. I think we can. In this document, Neil, I think that we can. We just right now have a singular line that says that the tiger team recommendations provide more detail on what makes choice meaningful, which includes that there's full transparency in education to the patient. That they understand what the implications of their choices are and that's completely under not really expressed at all in the PCAST Workgroup other than an acknowledgement that full transparency can be a challenge. But they go as far as to say that patients are going to largely self-educate, which is not what we said and that they would largely do this through a Web interface, so I think we can pull that out in some more detail.

Paul Egerman – Software Entrepreneur
Okay. That's excellent, Deven. It seems to me under better informed, meaningful consent that's a place where we want—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think sure transparency is part of it, but I totally agree with Neil; that it really is a huge issue regarding quality of care overall, because tagging individual data elements out of context has significant implications for care delivery.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I don't think this is where we want to spend our call today, but I'll register the other side is the consumer always has a choice of what they share with their providers and they don't always tell the full story and that's their choice. Sometimes they put themselves at harm for that, so that's the American way.

Paul Egerman – Software Entrepreneur
That's true. And these are excellent comments—again, to make sure we're framing the discussion correctly, we're not trying to discuss the merits of data element level security—

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Right.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Right.

Paul Egerman – Software Entrepreneur
We're trying to say how did this relate to our previous recommendations. That's, again, kind of hard because we're giving recommendations under like one set of circumstances and we're comparing a document that's written under different words and a different set of circumstances.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Paul, I mentioned at our last PCAST meeting that our tiger team's consumer choice hearing and then I sent an e-mail out to the members, directing them to the Web site where the testimony and send the conclusion. I think maybe we should make sure that people on the PCAST do understand what came out of that hearing.

Paul Egerman – Software Entrepreneur
Yes and that's a good observation and certainly it's a very good observation. Getting back to this document, under Better Informed, Meaningful Consent, if I heard your suggestion correctly, Deven—and trying to be also responsive to what Neil said—what's written here we need to expand a little bit in terms of the issue of patient education and the role of the provider. Also express somehow the information that Neil just described about the caution from the providers and concerns about this issue.

Deven McGraw – Center for Democracy & Technology – Director

Yes. No. I think that's right and we can go back, actually, to the text of our tiger team recommendations, both on meaningful consent, as well as granular choice where we had a lot of framing discussion about the very tension between giving patients more rights with respect to granularity of consent and quality of care and concerns on the part of the physician. So we can bring all of that out better in the version that we move forward and we'd be happy to take a stab at that and we can circulate it.

Paul Egerman – Software Entrepreneur
That sounds great. Thank you, Deven. So then moving on to Granular Consent, what is said here is interesting. The left cites page 46. The middle section, as I said before, makes our statement that we concluded that technology for granular patient consent is promising, but in the early stages of development. Then the analysis says, the tiger team recommendation could be read to be consistent with PCAST. That's interesting wording there; could be read to be consistent with PCAST if ONC pilots metadata tagging as an approach to implementing granular consent, because indeed, when we were talking about granular consent we certainly weren't necessarily talking about each data element or maybe we were. I thought we just meant granular, but—

Deven McGraw – Center for Democracy & Technology – Director
We did. I think we meant granular as in beyond just all in or all out.

Paul Egerman – Software Entrepreneur
Right. That's correct.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I have one observation that, again, is a little bit off topic from here. The PCAST model, the way I read it, seemed to imply that consent choices would be made at the time of the assignment of the metadata in terms of whether or not something was considered to be sensitive by the consumer. I think that's, number one, impractical and number two, it doesn't capture the notion that what you consider sensitive might change over time as your circumstances change. It's a PCAST issue per se, but it does affect the notion of granular consent as to when it's applied, what kinds of flexibility are given all, again, part of the complexity of granular consent. But I think our spirit, the tiger team's spirit was that you could change your mind as you either got more educated and realized it was foolish to restrict your data or your circumstances changed and you wish to restrict a different set of your data.

Deven McGraw – Center for Democracy & Technology – Director
That's right.

Paul Egerman – Software Entrepreneur
Is that still an observation about granular consent or an observation about consent?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
That's a good question. I think it's going to show up in the granular if we are trying to map to PCAST because they're talking about granular from the get-go.

Paul Egerman – Software Entrepreneur
Because it ... to me one place or the other, if I heard you right, David. That is the difference, which is that the tiger team recommendations were based on a concept that patient consent decisions could change over time—

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Could change, yes.

Paul Egerman – Software Entrepreneur
And that's unclear to the extent or how that happens in PCAST.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yes. I mean ... a bit of a notion of a static tagging that I think could perfectly well be implemented dynamically. It's a technical detail, but it's an important one when somebody gets down to actually building these things.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I think that the two—the notion has an interaction with the notion of granular so that it becomes a much more likely event that people would change a very granular set of changes when they got a new job, they decided to run for office, they retired, they became diagnosed with a chronic illness, all of the kinds of events we're talking about.

Paul Egerman – Software Entrepreneur
That's correct. You're right, Wes. Part of the information we got is as people got seriously ill they became sometimes less concerned about privacy, which is their choice, but it would be one reason why people might change decisions, privacy decisions.

I'm sorry. Was somebody else trying to say something?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I was just going to give the other example of this notion of static tagging is if you tag the data element as being visual acuity most people wouldn't mark that as sensitive until later in their life if they decide they want to be an airline pilot. At which point visual acuity is all of the sudden very sensitive to them.

Deven McGraw – Center for Democracy & Technology – Director
Right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
So that's the point I was trying to make. I think it's consistent with what Wes said too.

Paul Egerman – Software Entrepreneur
Yes, that's great. Thank you very much. Great comments. Looking at the issue of granular consent, what is written here is that the tiger team recommendations could be read to be consistent if ONC pilots metadata tagging as an approach to implementing granular consent.

Deven McGraw – Center for Democracy & Technology – Director
I think we might want to massage that a little to make it clear that when we talked about granular consent I don't think we conceptually thought of it as being sort of down to the atomic data level, whatever that means.

Paul Egerman – Software Entrepreneur
That's right. Deven, you're right, although it's really interesting when you read the report carefully it's not really clear how atomic PCAST is recommending, because it really talks about and uses the phrase more atomic.

Deven McGraw – Center for Democracy & Technology – Director
Right.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Right. But I think; this is—

Paul Egerman – Software Entrepreneur
Although I think there is an expectation more atomic is much more atomic.

Deven McGraw – Center for Democracy & Technology – Director
Right.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

In general there is a theme in the PCAST Report that documents our not sufficiently granular, so you could read more atomic as more atomic than documents without stretching, I think, their intent.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes. I would agree with that. I think it's possible to tag at a pretty granular level, even with the technologies that we have today, much less if we go and invent this universal exchange language, so you do have to consider that granular could be pretty granular.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Yes. Really, the biggest issue I think is that most of the thinking that's been done before, including by us, has been about algorithmically interpreting a statement of consent at the time data is retrieved rather than having that consent pre-attached. This is the issue we've gone over several times, but it also applies here in the sense that to the extent information is coded or we trust natural language processing we may have more difficulty in excising a document for specific things than we do if the data has been pre-atomized in the representation.

Paul Egerman – Software Entrepreneur
That makes sense.

Deven McGraw – Center for Democracy & Technology – Director
Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think it would be good for the tiger team to reflect that back to them rather than making assumptions of what PCAST meant, but really for the tiger team to make our recommendation on what granularity should make sense.

Deven McGraw – Center for Democracy & Technology – Director
Well, except that, Dixie, I think we're just trying to compare—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I know. Yes.

Paul Egerman – Software Entrepreneur
Yes.

Deven McGraw – Center for Democracy & Technology – Director
The things PCAST said with what we have already said versus further development on what's meant by data element level or how granular is granular. But I do think that rather than sort of just a blanket statement in this third column about there might be some consistency here if they took the piloting approach that we recommend. I think we've got to work this big to reflect the sort of richer dialogue that we just had in this section and that there sort of was much more to what we said on granularity and there is a lot of uncertainty in the PCAST Report. It's not clear exactly where the intersection is.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. Deven, that's what I was trying to say, but you did it way, way better. The other comment I wanted to say is that ONC just released some Challenge Grants that do address metadata tagging for privacy—

Deven McGraw – Center for Democracy & Technology – Director
Oh, okay.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
So where it says if ONC pilots, so they really have moved forward on that.

Deven McGraw – Center for Democracy & Technology – Director
Okay. That's good news. Thank you, Dixie.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Maybe this is nit-picky, but the phrase in the third column there, if ONC pilots metadata tagging, if the phrase metadata tagging means uses a newly created universal exchange language as specified by PCAST then I think we need to make that a broader statement here, because you could—

Deven McGraw – Center for Democracy & Technology – Director
Yes. We've got to broaden this statement. I think we're better off talking about how the tiger team recommended piloting technologies. I think the language, as is, has got to be changed.

Paul Egerman – Software Entrepreneur
Yes, I think you're right. David, I understand what you're saying about how it's written. It's not quite right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes.

Paul Egerman – Software Entrepreneur
I think you and I both understand what is intended to be said here, but what is written here is not quite ... so—

David McCallie – Cerner Corporation – Vice President of Medical Informatics
My point would be you could do granular consent on today's CCDs, because they are already tagged.

Deven McGraw – Center for Democracy & Technology – Director
Right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
That's just to say you don't need PCAST to worry about granular consent. We already have to worry about it.

Paul Egerman – Software Entrepreneur
That's right.

Deven McGraw – Center for Democracy & Technology – Director
Right. That's true.

Paul Egerman – Software Entrepreneur
I've just got like two or three minutes left in my time allocation—

Deven McGraw – Center for Democracy & Technology – Director
You can have a little bit more, Paul.

Paul Egerman – Software Entrepreneur
I'll quickly walk us through just a few more things. The part we just did is actually, in my opinion, the most challenging part to get the wording right and to express this. On security, again, there's a reference here of page 51, a general statement that says, "Well designed combination of encryption and authentication and so on." It lists that, although it does for—oops, why is—

Deven McGraw – Center for Democracy & Technology – Director
I'm sorry. That was me. I'm sorry about that.

Paul Egerman – Software Entrepreneur
Okay. I'm in a panic ... okay.

Deven McGraw – Center for Democracy & Technology – Director

Oops. I had turned it—Altarum, you might need to help here. I turned off the sharing because I was trying to get a popup off my laptop and I couldn't and we can't—

W
Did you need the PDF back on the screen?

Paul Egerman – Software Entrepreneur
Yes, please.

W
Okay. Great.

Paul Egerman – Software Entrepreneur
Okay. Fine.

Deven McGraw – Center for Democracy & Technology – Director
Thank you.

Paul Egerman – Software Entrepreneur
Perfect. So what it says here on security is again a summary, although there's actually a fair number of security statements in the PCAST Report that summarizes some of the things we've said and then it says, "Tiger team recommendations initially appear consistent with PCAST observations." There may be a need to further explore the particular approach recommended by PCAST. There's probably a reference there that's a somewhat complicated approach of what are the encryption keys or independent or de-coupled from the indexes.

What do we think about this statement or analysis?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Well, you know, I have been struggling to envision the PCAST approach operating with a high level of granularity and I think it's important to recognize that there is no disagreement on the fundamental need for encryption, authentication and authorization and that's entirely consistent with our report, with our work to date to the extent we've completed that work. But I'm having a hard time relating its notion of a digital rights management model for a complex set of options to anything we have written or considered, to be honest.

Deven McGraw – Center for Democracy & Technology – Director
Yes. Wes, I think that's a really good point. I think maybe we need to rephrase this analysis to state that certainly at the level of agreeing on the need for security control, such as encryption and audit trails and access we are aligned, but we didn't take up at all the detailed approach that they recommend.

Paul Egerman – Software Entrepreneur
Yes.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Right.

Deven McGraw – Center for Democracy & Technology – Director
Yes.

Paul Egerman – Software Entrepreneur
Yes. Since there may be dilution in there we say there is a need to explore the approach recommended ....

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Yes. I'd just like to strengthen that a little bit or somehow indicate the limitations on initially appear consistent.

Deven McGraw – Center for Democracy & Technology – Director
Okay.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I don't feel that they initially appear. I feel that there are many principles in common—

Deven McGraw – Center for Democracy & Technology – Director
Yes.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
But that there are mechanisms addressed in the PCAST Report that haven't been considered by this committee.

Deven McGraw – Center for Democracy & Technology – Director
Yes. Exactly.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
And then there are some things that the PCAST Report recommended that I think may in fact be un-implementable, although that's—

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
That's not a subject for us to discuss though, right?

Deven McGraw – Center for Democracy & Technology – Director
To talk about.

Paul Egerman – Software Entrepreneur
That's right. That's right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I'm just saying there's a lot more that needs to be studied here.

Paul Egerman – Software Entrepreneur
Yes. The un-implementable stuff is always—

Deven McGraw – Center for Democracy & Technology – Director
That's on your plate, Paul.

Paul Egerman – Software Entrepreneur
Absolutely. Absolutely. I hate it when they do that. So those are good comments about security in terms of we certainly agree with the baseline concepts, but the specific methodology that they described was not one that the tiger team has evaluated and it does need evaluation.

Authentication is actually something that we hoped to start talking about in this call. It's like, I think, predominantly authentication for users, but also for patients as really all participants, but we haven't really done that yet, at least on an individual case, so I'm going to skip past this one right now.

Third Parties: Do you want me to keep going, Deven, on this or do you want to switch?

Deven McGraw – Center for Democracy & Technology – Director
No. No. No. Go ahead. That's fine.

Paul Egerman – Software Entrepreneur

Okay.

Deven McGraw – Center for Democracy & Technology – Director
I mean unless you need to take a break.

Paul Egerman – Software Entrepreneur
No, I'm fine.

Deven McGraw – Center for Democracy & Technology – Director
Okay.

Paul Egerman – Software Entrepreneur
Third Parties: This is interesting. PCAST talks about DEAS operated by states and possibly large healthcare delivery networks or the private sector. They try to line that up with our recommendation, the tiger team's limitations on third parties' collection, use and retention, which I think makes sense. Basically, the analysis is that the tiger team recommendations are more detailed on limits on intermediaries. It says, "The tiger team may want to consider the implication of the DEAS proposal on transparency recommendations.'

Do we have any comments about what's written here?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I think the notion that DEAS will not have access to personally identifiable health information is a questionable assumption, but that's a DEAS problem.

Paul Egerman – Software Entrepreneur
That's a different issue.

Deven McGraw – Center for Democracy & Technology – Director
Yes. I mean that is what they say in the report, but know a number of people have raised those questions.

Paul Egerman – Software Entrepreneur
But this topic is really sort of like the third parties themselves, the organizations themselves that run like the DEAS or the record locator service.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes. Yes.

Paul Egerman – Software Entrepreneur
So we did make some recommendations about the responsibilities of those third parties. To me—and we put some detail limits on that, so we have much more detailed information, but as it says here, the DEAS is sort of like a different animal that we would have to consider, but I don't see that what we said about the third parties' obligations are inconsistent with what PCAST is saying.

Deven McGraw – Center for Democracy & Technology – Director
Yes. I think it's too hard. I mean there isn't an obvious conflict, but they said so little about how these DEASes would be governed and what sort of rules would apply to them that it's hard to know, but at a minimum we certainly set out some pretty good, strong recommendations on the way that intermediaries, like an access service, what their responsibilities were with whatever data they did retain and they shouldn't be retaining any data they don't need or collecting what they don't need to perform that function. So we said that and I think that was the point that we want to make most clearly is that in any discussion about models of query and who's going to provide that access or index, our tiger team recommendations should be relevant there.

Paul Egerman – Software Entrepreneur

Yes. That makes sense to me.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes. I agree that as an intermediary that holds, potentially holds PHI they have to follow the same rules as any other intermediary.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think this is really the crux of where the inconsistency – well, not really inconsistency, but problems may arise because as I recall all of our discussions about the shifting of control when control over the data and even the linkages, all of that intermediary discussion, I believe that's where we said it requires the individual's consent. I think if you required, if you superimposed individual patient consent over the DEAS model that PCAST recommends, I think it would significantly constrain what they have in mind.

Paul Egerman – Software Entrepreneur
That could be, although again, returning to what it says here—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's what I'm talking about, what it says there.

Deven McGraw – Center for Democracy & Technology – Director
Well, although they actually do give patient consent rights with respect to DEAS and we took care of that. We sort of separated that analysis from the notion about what are the sort of baseline fair information practice rules that ought to apply to intermediaries.

Paul Egerman – Software Entrepreneur
Yes. This is just one of the rules that apply to these other organizations, the state organizations or possibly the health delivery networks or possibly the private companies that might be running these DEAS services.

Deven McGraw – Center for Democracy & Technology – Director
Right. Well, and to the extent that there is a consent policy that they need to follow that would be part of the rules, but we sort of have that covered, I thought, in another category.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That we've already discussed?

Deven McGraw – Center for Democracy & Technology – Director
Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I didn't get that. So let me ask a question.

Deven McGraw – Center for Democracy & Technology – Director
This was the whole discussion, Dixie, about whether the DEAS was like a trigger circumstance under our consent recommendations.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Okay. Yes. You're right. That's where it's at. Yes. So you believe it does require—yes, that's right. We did have that other. Yes. So it does require patient consent and I remember we had it. Yes. So it does require patient consent even to have your information indexed by the DEAS. Is that your understanding?

Deven McGraw – Center for Democracy & Technology – Director
I think that's right in the PCAST Report.

Paul Egerman – Software Entrepreneur

Yes. The PCAST Report says patients are not required to participate in DEAS. They can choose either some data elements or, I guess, altogether not to participate.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Okay. My apologies. I thought it—

Paul Egerman – Software Entrepreneur
Getting back to this issue, basically the way I look at the PCAST Report on third parties is it says third parties can offer these DEAS services, but it doesn't really say too much about the third parties' obligations as a consequence. That's what we provide when it says there is more detail. Any other comments about this on third parties?

The final category is Patient Linking. There it is in PCAST. There is reference to page 42, a fair discussion about the patient linking process and talks about statistical methodologies in the middle column. There is a description a little bit of what we did with our patient matching hearing and the analysis is that on this topic they seem to be consistent. Although there is a comment that you might need to explore some of these issues further when more is known about how the PCAST recommendations are to be implemented, which is probably true. Any comments on this issue?

Deven McGraw – Center for Democracy & Technology – Director
Yes. I think that's right. I like the way it's framed as the direction of our recommendations, because we sort of stress different details in what we put out.

Paul Egerman – Software Entrepreneur
That's the last item in the—

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I'm sorry. I didn't speak fast enough here. I believe that our testimony left us less sanguine about the possibility of matches suitable for all purposes than the PCAST Report was and significantly so.

Deven McGraw – Center for Democracy & Technology – Director
Right.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
So again, saying that in a sense that they may need to explore these issues further, I mean some of us were in a discussion with some of the principals of the PCAST Report. And they clearly have different information than we do about the likelihood of what is usually called master data matching across industries, as being sufficient for healthcare. So I would like to say that I just don't think we can fairly say it appears consistent with PCAST. I think we need to find another way of wording this just the right amount more strongly in order to; perhaps Paul or Deven could just look at how we worded the other one and suggest an alternative wording, but—

Paul Egerman – Software Entrepreneur
I wonder if you could also help us with that, Wes. I mean you're 100% correct.

Deven McGraw – Center for Democracy & Technology – Director
Yes.

Paul Egerman – Software Entrepreneur
I like your expression less sanguine.

Deven McGraw – Center for Democracy & Technology – Director
Yes.

Paul Egerman – Software Entrepreneur
But yes, there is a difference there and so we should articulate that.

Deven McGraw – Center for Democracy & Technology – Director
Yes. I think we need to articulate the particular point you raise, Wes, about how we heard very clearly in testimony that the rate of accuracy and whether you error on the side of false positives or false negatives is going to vary based on a number of factors and the PCAST Report assumes a bit of a one-size-fits-all approach.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Yes and in the discussions, they've heard from people, who we didn't hear testify and who have presumably a specific experience base that it would be good to compare to the experience base of our folks and try to rationalize or reconcile difference, but I think we need to state that as a step that needs to happen.

Deven McGraw – Center for Democracy & Technology – Director
Yes.

Paul Egerman – Software Entrepreneur
So those are all excellent comments and this was the last one in the report in this analysis. So here's what I would like to suggest we do next: Deven and I, and we'll probably reach out to a few of you, like Wes and Dixie, will work with the people at MITRE and see if we can alter this document to reflect the various comments. Then we'll send it out and give you some time also to go through it yourselves carefully and make any additional adjustments.

In other words, it's not like there's a huge sense of urgency, although we would like to get this done within the next, say, two or three weeks. So there's a little bit of urgency on it, but we also want to make sure you have a chance to go through it carefully and make sure everybody is comfortable with it. It's an interesting discussion as I reflect on what we just walked ourselves through besides understanding the PCAST Report it's given us a chance to actually remember all of the recommendations that the tiger team has made. As you look at it, we've done a lot of work on a lot of these important topics, so I think it's a great discussion.

Deven, are we ready to move on to the next topic, unless somebody else has—?

Deven McGraw – Center for Democracy & Technology – Director
Yes. I mean I think I am unless someone has something else they'd like to share on that. I think it's a good plan, although let me ask one question of you, Paul. I don't want to push people unnecessarily in terms of the time we need to take to get this finished and get our discussions accurately represented, but is there a reason to try to have this available before the hearing or the—

Paul Egerman – Software Entrepreneur
I would just tell you it would be helpful to do that. I mean the way the hearing works is—to make sure everybody is on the same page—the PCAST Workgroup is holding hearings on February 15th and February 16th. It is being held jointly with all of the members of the Policy Committee and all of the members of the Standards Committee, so there will be a lot of people there. The way the days are structured, February 15th is really all testimony. Right now, February 16th is a half-day and what we're going to be doing on February 16th is discussing material. The first topic is probably going to be trying to come to some consensus of whatever it was that we heard on February 15th, but the intention of what we're trying to do with the PCAST Workgroup February 15th is sort of like the half-way point in our deliberations.

Everything up to February 15th is like information gathering. We're trying to make sure everybody understands the report, gather as much information as we can from the public and from various sources. Then on February 16th we're trying to analyze what we understand and we're going to roll up our sleeves and say, "Okay, now what's the impact on ONC and ONC programs?" And start saying, "What does this to stage two of meaningful use? What does this do to the HIE programs?"

The reason why I'm saying that is to the extent that we get this done by February 15th or February 16th then that's consistent with the workgroup's schedule of gathering information. It's not terrible if it's a little bit late, because we're going to have so much information, but that would be ideal if that were possible.

Deven McGraw – Center for Democracy & Technology – Director
Okay. Well, let's try. That starts with you and I sort of turning around sort of an initial cut at some changes, which I think we'll aim to do for early next week, so keep an eye on your inboxes.

Paul Egerman – Software Entrepreneur
Great. Good discussion. Thank you, everyone.

Deven McGraw – Center for Democracy & Technology – Director
Yes. No. It was a very good discussion. I want to pat everyone on the back for largely keeping the discussion of PCAST closely focused on the intersection with the tiger team recommendations. I think there are a lot of things that I know many of us want to say and share about the PCAST Report in general and I thought we all did a really admirable job of keeping a pretty focused discussion.

So I want to take a couple of minutes to talk a bit about the future plans of the tiger team and issues that we will take up in both the short-term and the longer-term. You did receive in your e-mail from Judy, but clearly not with sufficient time to digest it and that's okay. An analysis that we've begun to do of gaps in the policy framework that we are trying to populate, keeping in mind that we have this set of principles that were adopted by ONC as part of the overall strategic plan and that were also endorsed by the Policy Committee. All of our efforts on all of the issues that we have taken up on an issue-by-issue basis have been aimed at populating an overarching and comprehensive framework of policies that further flesh out and develop those principles.

So what we've tried to do in the policy framework document—I think it's described in the download list as a meeting planner—is to highlight the recommendations that we've put in there to date and an initial sketch of where there might be gaps. But this area in particular is where we really want to hear from the members of the tiger team about what other issues you think we need to discuss and where you would put that in terms of priority order, if you think we need to do something sooner rather than later. I mean we have, in large part, been responding to the needs assessed by the Office of the National Coordinator and the staff there about what issues that they need us to focus on, which I think is right, because I think we need to be responsive to what their needs are from a programmatic perspective. But I don't want us, as a team, or the Policy Committee or even the public, who is following our work, to think that there is not an overall plan here or an overall strategy and to understand where each of the issues fit within a broader effort that we're doing, again, to populate this framework.

This is not as much of a time sensitive issue. I think we can take some time with this. So while we're going to ask you over the next week, maybe week and a couple of days, to pay attention to finalizing this PCAST Report document that we just spent so much time discussing, I also want to put on deck for you helping to identify the gaps in terms of policy issues that we have yet to take up and that we need to take up in order to populate this framework.

But we do actually have issues teed up through April and they are largely issues that we have had either on the back burner for some time, which one of them being issues related to patient access, which include identification and authentication, but we also have been asked by the Office of the National Coordinator to consider user authentication. I'm sure you all remember that we did put up a set of recommendations on authentication of provider entities, so for entity-to-entity transactions, machine-to-machine handoffs. We put a set of recommendations in place, but we did not drill down at the individual user level and we have been asked to consider whether there are some circumstances under which we would want to make policy at an individual user basis. So what I think we hope to do in this call, because we are really only beginning our discussion, is to try to sketch out some parameters for the user authentication discussion. In other words, what are the set of use cases or circumstances where we would want to establish some clear policy on user authentication down to the sort of individual level.

Paul, before we turn this over to MITRE to sort of take us through some background slides I want to make sure that I've articulated the direction we're heading in.

Paul Egerman – Software Entrepreneur
Yes. Great job.

Deven McGraw – Center for Democracy & Technology – Director
Does anybody have any questions about the sort of population of the gap analysis document or where we're heading next? So in other words, we're starting with user authentication not at the patient, not patients as users, but individual providers or clinicians or staff within a hospital. But we do have teed up to follow on after completing the provider side of user authentication the patient access, patient identification and authentication issues that we have kind of had in our parking lot for a long time, but we've been asked to do provider user authentication first by ONC.

With that I'm going to turn it over to Jay Brennan of MITRE, who I think is our MITRE person, who is going to take us through some background slides.

Jay Brennan – MITRE
This will be very brief, Deven. Thank you. I'm on slide three because you've covered slide two for us. This is a little bit of a refresher and then we'll cover a few things about what the government says about authentication. Slide three is just a reminder of where authentication fits in things. We're going to give somebody or the idea is to give somebody access to healthcare information. Authentication is one of the steps in the whole train of events that leads up to granting access, but it's a very important one where we actually verify that the claimant, somebody whose claims that they should have access to healthcare data actually is the person they claim to be.

If you can advance the slides to number four? We've covered authentication and for the purposes of discussing this—and I'm not wed to the word token, but—we will just use the word token. It's a term of art. People argue about this term of art and so we should get it out of the way and not argue about it and just accept it for Friday. If you want to do something different on Saturday that's great, but for the purposes of authenticating what we want users to do is to prove that they possess one or more tokens. What are these tokens? Well, they're things like passwords. They're key fobs. One of the things that is used in various places are things called Bingo cards, where you get a grid full of numbers and the authentication process asks you to provide the number that's in row three and column four. These would be mailed to you. That's one possibility. Biometrics; you scan your finger. There are a variety of ways that authentication can be implemented by the use of tokens.

The reason why this is important here is that the confidence we have in the proof of the identity of the person can be linked to how many factors they use. Now, this is not a mathematical proof that says if you use three factors that's mathematically better than two, which is mathematically better than one. That's not it. General, accepted practice is that if you use three factors that's better; you have more confidence than if you use two than if you use one. That should be understood here up front. This is not a written law that says two-factor is better than one. It's generally accepted practice that it is.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Question.

Jay Brennan – MITRE
On the next four slides, if you move on to slide five—

Deven McGraw – Center for Democracy & Technology – Director
Jay, you have a question. Go ahead, Wes.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

So it's usual to hear tokens subcategorized into something you know, something you have or something you are and to impute a different level of assurance of the authentication when they're mixed. Is that a concern in this discussion?

Jay Brennan – MITRE
It's a concern if you want to make it. I think what you can say in general is these factors should be independent of each other, but that does not say that you could not have two, say, knowledge based tokens in the same authentication. Again there is no rule here, but when I go look at the draft missed specifications, for example, it's perfectly acceptable in the draft, in their new draft, to have two that would be knowledge based. So you could answer questions that were prepositioned knowledge that you would have about what's your favorite car, what was your first girlfriend's name and then a password. So those things would be sort of independent of each other. I think the key is independence as opposed to trying to say something that says one has to be a bio and one has to be something you know.

On slide five, HIPAA has something to say about access to healthcare data. If you look at the lower left it basically says that you need to put in place a procedure to prove that the person, the claimant is actually who he or she says they are, but they don't give any specific rules on how to do that or mandate anything. That's the key point from HIPAA.

On the next slide, PCAST says all of these methods are acceptable, but again, doesn't give any specific direction on which method would be most acceptable or any circumstances under which one method would be used in preference to another. Again, two-factor authentication is impossible to design choice according to PCAST

If you look on the next slide—

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Can I interrupt for a question?

Jay Brennan – MITRE
Sure.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
We are potentially addressing this provider authentication not just in the context of PCAST, right?

Jay Brennan – MITRE
Sure. Yes.

Deven McGraw – Center for Democracy & Technology – Director
Yes. Absolutely.

Paul Egerman – Software Entrepreneur
The purpose of showing that is just to give you additional background information.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Okay. I just wanted to make sure it wasn't constrained to just PCAST.

Paul Egerman – Software Entrepreneur
No. This is what PCAST says. This is what OMB says. This is just background information and also the very subtle thing, David, you said provider authentication. I suggested that we call this user authentication—

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Good point.

Paul Egerman – Software Entrepreneur

Because I think you know a little bit of ambiguity about what you mean by providers, but it's also not just clinicians or individuals.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Right.

Paul Egerman – Software Entrepreneur
There could be non-medical staff access.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes. That's a great point. I was thinking non-consumer, but you're right, user.

Deven McGraw – Center for Democracy & Technology – Director
Yes, it's tough when you get to user, but that's the word we're using for now, user.

Paul Egerman – Software Entrepreneur
Yes and I don't know if that's the right word, but it's individual users of the EHR system.

Deven McGraw – Center for Democracy & Technology – Director
Right.

Jay Brennan – MITRE
Slide seven then summarizes the missed authentication guidelines that appear in the SP-863. You can see going across the top that three of the four levels; the fourth level isn't shown because it's well beyond anything anybody has discussed for healthcare in most circumstances. The second row there in that matrix shows you the sort of subjective wording around the level of confidence you have at each level. There is little, some and high confidence if you use none, single or multi-factor authentication. Again, this is subjective and we're working under the belief that multi-factor is always better than single factor.

The next slide is the final one of the quick government survey and that is OMB guidance on this. It basically says for agencies to allow people to have access, remote access that is and they don't really actually define what remote access is in this particular guidance, but we can assume it's not at the mother ship, whatever the agency sets up as agency headquarters or the agency building or the agency network, you're not there. You're somewhere else and so from that somewhere else place, in order to get into the agency it's very important to understand that this guidance is really talking about people who are getting access to the agency as if they were there, which is an important distinction to make because not all remote access is as if you were there. But in any case, OMB says if you're getting access from a remote location into an agency then it has to be two-factor or at least they suggest that it would be two-factor. There is, again, no hard and fast rule.

That's the quick survey of the government stuff. We're going to turn this back over to you, Deven, at this point to cover the previous tiger team—

Deven McGraw – Center for Democracy & Technology – Director
Okay. Great. Thank you, Jay. That was really helpful. Thank you for joining us on this call and hopefully subsequent calls, because a lot of this discussion is going to have some important technical dimensions and we have, I think, a good degree of technical expertise among the members, but it's always helpful to have some more. Thank you very much.

I want to remind everybody about the previous tiger team recommendation that was made in the collection of recommendations related to provider entity authentication. What we said at the time was that with respect to individual users provider entities and organizations must develop and implement policies to identity proof and authenticate their individual users, which is already required under the HIPAA security rule. I think that what we intended here—although this is the reason why we're raising it on the call—was that with respect to the operations within a physician practice or within a hospital we were not comfortable with telling these institutions specifically what they were required to do beyond what the security rule already requires them to do with respect to authenticating their individual users. I think that we really had in our mind this sort of internal enterprise access, as opposed to thinking of what happens remotely, such as what was addressed in OMB's policies or kind of other models of record access, including, but certainly not limited to the particular model that the PCAST is exploring. I don't think we shut the door, in other words, on user authentication, but we did say clearly to the Policy Committee that we thought that the policy under the security rule that required implementation of user authentication policies within an institution or within a provider's walls was sufficient from a policy standpoint.

So, assuming that we've already made that recommendation I think that raises an important set of questions, which is what are the circumstances under which we think there ought to be some more specific policy with respect to authentication of users. I'm going to turn it over to Paul. We teed up some discussion questions here just to really get this conversation started since we don't have as much time left in this call, but we wanted to get some stuff out on the table that are related to defining the parameters of what we would want to make policy on.

Paul Egerman – Software Entrepreneur
Thank you, Deven. Here are the questions: They're sort of laid out here in bullets, so I'm going to sort of go through this in one shot and then ask for people's comments. The first question is should we be making any policy recommendations at all related to user authentication? That's one idea.

The second is maybe we should, but essentially maybe it's when the user if physically outside of their organization. Or maybe another way to look at this concept of remote access might be to say maybe the policy is related to when the user is accessing the EHR over a public network, a public network probably being the Internet, but just over a public network. Maybe we make that as the area we want to deal with. Then once we decide that the question is should the tiger team make recommendations on the level of authentication, single-factor versus two-factor and whether or not we should make recommendations on specific methods of authentication of users.

Maybe there are even more questions, but let me pause there and see how people react.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
A question that has come up quite frequently in the area of HIEs and other kinds of information exchange is the degree to which the identity of the user—okay, I'm going to back off. That's really not about authentication. I apologize.

Deven McGraw – Center for Democracy & Technology – Director
Okay.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I certainly think that it makes sense for the tiger team to weigh in on this just in terms of question number one. Not doing so would be a little bit like putting on a warm coat and forgetting to zip it up.

Deven McGraw – Center for Democracy & Technology – Director
A timely comment given the weather lots of people have been experiencing.

Paul Egerman – Software Entrepreneur
Yes. David, you are terrific when it comes to those comments. It's unbelievable. That's great. So you say yes we should.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes.

Paul Egerman – Software Entrepreneur

And the fact that we've got this here is ONC would like us to do this, to address it, but we just wanted to make sure that the tiger team wants to do that, because in previous discussions there was some feeling HIPAA is covering this and maybe we shouldn't touch this thing.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Well, since that time the FDA has implemented their regulation regarding e-prescribing for controlled substances, so since the tiger team made that recommendation we have at least one use case, which does require two-factor authentication.

I would further say—and David's analogy with the open coat makes sense, but I think this tiger team should make a very firm statement that recognizes the fact that authentication is kind of the long pole in the tent when it comes to security. Because access control and audit and so many other security, just literally even digital signature, so many other security protections rely on it that if there is one area at all that we should make recommendations then I think this is it.

Paul Egerman – Software Entrepreneur
Okay. For two people to say yes we should do this, does anybody want to say no, we should not do it?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I'm going to create a reservation, but not actually disagree. This is Wes again. I guess, first of all, on the agreement side the lack of specificity in this area has been a thorn in the side of everyone who is trying to be compliant in good faith, but focus on getting whatever their actual job is done where the job isn't actually security; it's taking care of patients or something like that. So the degree to which we can create some specificity would be a boon to the industry.

The down side of that is that the lack of specificity—any recommendation that is specific is bounded in time because new technologies come into place. New appreciations for the importance of security come into place that increase user tolerance for existing technologies. There are all kinds of reasons why in an environment that moves as slowly as regulation does it's hard to be specific. So I think we have to either find, we have to address both specificity and evolution over time in any recommendation that we make.

Joy Pritts – ONC – Chief Privacy Officer
Wes, I hear you loud and clear and I think that's why the original rule was written so that it's scalable and flexible, but there are other means of even just putting the specification into a regulation that you can accomplish the same thing. I'm not saying that we would do this, but this is just a way people do accomplish that is through issuing guidance, which is a way of telling organizations that if you were to do certain things that you would be in compliance with the more general regulation.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Well that's really great to know. Maybe we should frame an early discussion on this point around exactly that. If there is any more complexity than just regulation and guidance, perhaps understanding what options are available to ONC would be helpful to us in not being afraid in going forward with specificity.

Joy Pritts – ONC – Chief Privacy Officer
I think that one way of approaching this is to know that there are other means that are available. And for the group to focus on the general premise that we want this to be something that applies now, but not necessarily forever and incorporate the flexibility aspect into the recommendations rather than this group try to figure out what the appropriate lever might be.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
How are the NIST recommendations treated with respect to the notion of guidance? I think that those NIST documents are just flat out brilliant at the way they create categories, but leave it open as to the definition of technologies that can meet a particular category. Can we follow that rubric or even reference those documents?

Joy Pritts – ONC – Chief Privacy Officer

It becomes pretty complicated because; I'd have to check on that; at least in a regulation we have to refer to a specific material that's in existence, so you can't say, "Gee, just follow NIST in whatever they do going in the future and you'll be fine."

Deven McGraw – Center for Democracy & Technology – Director
But in terms of specifically referencing the SP blah-blah-blah document that Jay walked us through, since that is a specific document does that count if we wanted to endorse the NIST recommendation for a particular set of—

David McCallie – Cerner Corporation – Vice President of Medical Informatics
... guidance ….

Joy Pritts – ONC – Chief Privacy Officer
I think that if you look to the guidance that was issued for breach notification that that might be helpful in knowing how to frame this because that was approved, right? It went through clearance already.

Deven McGraw – Center for Democracy & Technology – Director
Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
This is Dixie.

Paul Egerman – Software Entrepreneur
Just a second—to get back to the question and I'll get to you in a minute, Dixie—the question is should we be making recommendations about user authentication and what I'm hearing so far is everybody is saying yes. Wes appropriately pointed out that we have to do it in such a way that we don't like cast this thing in concrete and create a problem.

Joy Pritts – ONC – Chief Privacy Officer
Yes.

Paul Egerman – Software Entrepreneur
Okay. So that's going to be a consideration, to make sure that we're not carving it in granite, although I should let David McCallie come up with a better metaphor, but that I understand. But so far I'm hearing everybody is saying yes, we should do this.

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist
Paul, I'm just curious about the scope of what kind of discussion you're interested in, because you used the term electronic health information, which is a very broad term. I was just wondering if you were seeing it more so limited to electronic health records and health information exchange, which may be a very different use case than, say, checking a calendar remotely that may have some electronic health information in there.

Paul Egerman – Software Entrepreneur
Excellent question, Adam. My assumption, which may be wrong, was that this was authentication for users or EHR systems, either in general or perhaps very specifically for certified EHR systems. Maybe I'm wrong in making that assumption.

Deven McGraw – Center for Democracy & Technology – Director
I think it's one of the things that as we sort of dive down into defining the particular areas, assuming that we want to do some boundary scoping here about what we're talking about that that's an issue that we probably will want to take up. The issue of not just the circumstances under which we think there ought to be some more clear policy and requirements on user authentication, but also what types of information access are we talking about.

Paul Egerman – Software Entrepreneur

Yes. I mean it's a great question because also, even if you assume for a moment and maybe it's a jump to say this, but my assumption is that it's the EHR system; the question is what's the EHR system? Is a lab tech putting a vial of blood into a machine that creates the laboratory results automatically? Is that data entry into the EHR system? Do we apply it to that technician? So we need to describe the scope of that. I think it's a great question.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I wanted to make two comments. Number one is regarding Wes' comment. I think at the policy level there is very little risk here that we're going to get out of step with technology because authentication technology, two-factor, which is something you know, something you have, something you are has been around for decades at the policy level. Where the risk resides is more at the standards level, I believe.

Secondly, regarding NIST 800-63, we actually—David will remember this—the Privacy and Security Standards Workgroup wanted to include that in our recommendation in the regulation and we were told we could not cite a NIST document as the standard for a regulation that was being posed outside of the federal government. That's what we were specifically told. As I recall, and I can verify this, but I do know that the first version of the e-prescribing of controlled substances regulation did cite NIST 800-63 and I believe that the final rule took it out. I presume for the same reason.

Paul Egerman – Software Entrepreneur
That's helpful. So on these four questions that are on the screen, I think we've answered the first question with yes.

The second question relates to do we want to constrain this a little bit? When a user is physically outside of their organization or maybe another way to look at it is do we want to say when a user is physically inside their organization, if they're within, say, a hospital and also assume for a moment that there is no public network involved. They're in a hospital; they're at terminals connected to an in-house computer system; maybe it's not connected right to the server and they can actually physically see the server, do we want to carve that out and say we don't want to deal with that or do we want to say we're going to deal with all users. We could say we want to deal with remote access, which is written here, but another way to look at remote access is we could say we want to deal with situations where a public network, presumably the Internet, is involved.

Deven McGraw – Center for Democracy & Technology – Director
If I can just add on to that for a second, the reason why we're asking about sort of defining some parameters here is because we had in our previous discussions on provider entity authentication expressed a very clear preference for allowing institutions and provider practices for example to determine what their mechanisms were for authenticating individual users. I sort of remember even some of the statements that were made on those calls that we're not going to tell hospitals what to do with their staff. So while I think I assumed that given those, what felt to me at the time like some pretty strong resistance to setting some more specificity around authentication, at least internally, what does that mean for what we think needs policy beyond that? Or do we want to reassess that recommendation in light of some other developments?

Does everybody need some moments to think about that?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Your sentence was so long that I lost that recommendation in the context.

Deven McGraw – Center for Democracy & Technology – Director
I'm sorry. Let me see if I can go back to it.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Okay. Thank you.

Deven McGraw – Center for Democracy & Technology – Director

Yes. I mean this is in the slides. I'm on slide nine for those of you who are not on-line. We said when we provided our provider entity authentication recommendations to the Policy Committee, which were endorsed, with respect to individual users, entities and organizations must develop and implement policies to identity proof and authenticate their individual users, which is already required under the HIPAA security rule as Jay pointed out. We didn't want to say more than that, such as recommending two-factor authentication for example.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Within an organization?

Deven McGraw – Center for Democracy & Technology – Director
Well, I think we meant within an organization and so if in fact that is what we meant when we said this what are the circumstances where we think we do want to provide some more policy direction? Maybe that is, as Paul laid out in the discussion, it's an inside-outside question and then what does it mean to be inside versus outside? Is it about physical presence? Is it about some sort of network, which is more subject to public access versus a virtual, private network? What are the parameters under which we think there ought to be more said than is already in the security rule about individual access?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Okay. I have one that I would like to put on the table and that is when a single sign-on is involved, especially single sign-on between entities where we have standards out there that will pass and authenticate an identity. If I'm authenticating ... and want to pass it over I think we should recommend, we should—

Paul Egerman – Software Entrepreneur
I don't mean to interrupt you, Dixie; that's an excellent topic, but I think you're a little bit ahead of us.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
No. I'm just putting it as one area I think we should consider. In other words, I think it should be another e.g. there.

Deven McGraw – Center for Democracy & Technology – Director
Oh.

Paul Egerman – Software Entrepreneur
Okay. I guess perhaps I'm not asking the question correctly. Basically the question I'm asking is should we be talking about all user access or should we limit ourselves to access that is done. This is written like remote use, but it could also be viewed as any access over a public network—

Deven McGraw – Center for Democracy & Technology – Director
Or the between entity example that—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think we should, at this point, include everything, but when we get down to really recommending a policy we, at that point, could say, "Well, within an organization it's up to them," but for now to decide—

Paul Egerman – Software Entrepreneur
Okay.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Do we have an ask here? I mean I think that opening the topic of user access within an organization would be valuable to the industry if there's an ask to do that. If nothing else, we could become the thing that everybody shoots at so we can figure out what size bullets they're shooting. But only if the output of that is actually something that ONC is looking for and prepared to use in some substantial situation.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Like EHR certification.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Or HIE certification.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Right.

Deven McGraw – Center for Democracy & Technology – Director
Right.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Yes, but I just want to make sure there is an ask for that at that level of intra-organization as opposed to HIE, which is internal organization.

Paul Egerman – Software Entrepreneur
Yes. That's a good question. I don't know.

Joy Pritts – ONC – Chief Privacy Officer
The ask was focused on exchange—

Deven McGraw – Center for Democracy & Technology – Director
Yes.

Joy Pritts – ONC – Chief Privacy Officer
But with the recognition and I don't know how you draw this line, but part of the concern for this discussion came from remote access, particularly from a provider's office to a software-as-a-service where there was concern voiced by many that just a password may not be sufficient for that sort of transaction.

Paul Egerman – Software Entrepreneur
That's helpful, Joy. What I would suggest based on these comments is that our starting point for a discussion could be what I call the public network, which would take care of the software-as-a-service situation. We'd take care of the remote access and the exchange situations. That becomes like the starting point. In some sense, I think there are different security challenges there, but what do people think of that?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Well, yes, as long as we define what public network meant.

Deven McGraw – Center for Democracy & Technology – Director
I think we would have to.

Paul Egerman – Software Entrepreneur
Yes, we're going to define that, but you have to find out about everything. What does remote access mean?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I wonder if this notion is more along the lines of access from an environment without controls, access to machines or something. It's not so much that it's going over the public network as it is that the location you're doing the access from has not validated who you are in any way. I mean our clients communicate to us with packets that go over the public Internet, obviously deeply encrypted, but nonetheless, it's a

public Internet. But what's different is that you can't walk into the nursing station and access the computer because people will stop you.

Paul Egerman – Software Entrepreneur
That's right.

Deven McGraw – Center for Democracy & Technology – Director
Right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Whereas, someone sitting at home using that very same network is in a different mode because no one has screened them before they got to the device. It's subtle. I don't know.

By the way, unfortunately, I'm going to have to log off. I have to go do an interview and I've got to travel a few hundred yards here.

Deven McGraw – Center for Democracy & Technology – Director
That's alright. We are reaching the point of the meeting to end anyway. This is the beginning of a longer discussion on this.

Paul Egerman – Software Entrepreneur
Yes, so this is good. We'll try to synthesize this between remote access, public networks and what you just said about the identity. Let's see if we can figure out a way to write that, but that should be the starting point for our discussion on the user authentication I think.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Great.

Paul Egerman – Software Entrepreneur
Terrific. Great discussion. Actually a range of topics today, but I think we're ready to do the public comments. Do you have anything you want to add, Deven?

Deven McGraw – Center for Democracy & Technology – Director
No. Public comment. We're ready.

Judy Sparrow – Office of the National Coordinator – Executive Director
Operator, can you check and see if anybody wishes to make a comment to the tiger team?

Operator
We do not have any comments at this time.

Judy Sparrow – Office of the National Coordinator – Executive Director
Okay. Thank you. Thank you, everybody.

Paul Egerman – Software Entrepreneur
Yes. I'll just say thank you, everybody. I hope everybody follows David McCallie's suggestion and keeps their coats—

Deven McGraw – Center for Democracy & Technology – Director
Zipped up.

Paul Egerman – Software Entrepreneur
We're moving forward anyway. Great discussion. Thank you very much.

Deven McGraw – Center for Democracy & Technology – Director
Yes, thank you everyone.